开源治理服务

常见问题

文档版本 01

发布日期 2024-03-13

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 二进制成分分析类

1.1 成分分析的扫描对象是什么?

成分分析的扫描对象为产品编译后的二进制软件包或固件：Linux安装包、Windows安装包、Web部署包、安卓应用、鸿蒙应用、IOS应用、嵌入式固件等；不支持扫描源码类文件。

1.2 成分分析的主要扫描规格有哪些?

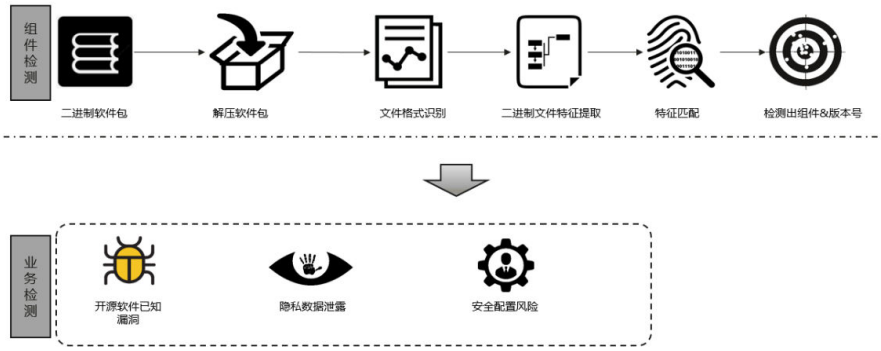
- 支持的编程语言类型：C/C++/Java/Go/JavaScript/Python。
- 支持的文件：.7z、.arj、.cpio、.phar、.rar、.tar、.xar、.zip、.jar、.apk、.war等格式文件，及Android OTA Images、Android sparse、Intel HEX、RockChip、U-Boot等固件。
- 支持上传的文件大小：不超过5GB。
- 平均扫描时间预估：根据不同的压缩格式或者文件类型扫描时长会有一定的差异，平均100MB/6min。
- 服务采用基于软件版本的方式检测漏洞，不支持补丁修复漏洞场景的检测。

1.3 成分分析的扫描原理是什么，主要识别哪些风险?

对用户提供的软件包/固件进行全面分析，通过解压获取包中所有待分析文件，基于组件特征识别技术以及各种风险检测规则，获得相关被测对象的组件BOM清单和潜在风险清单。主要包括以下几类：

- **开源软件风险：**检测包中的开源软件风险，如已知漏洞、License合规等。
- **安全配置风险：**检测包中配置类风险，如硬编码凭证、敏感文件（如密钥、证书、调试工具等）问题、OS认证和访问控制类问题等。
- **信息泄露风险：**检测包中信息泄露风险，如IP泄露、硬编码密钥、弱口令、GIT/SVN仓泄露等风险。
- **安全编译选项：**支持检测包中二进制文件编译过程中相关选项是否存在风险。

图 1-1 风险项



1.4 成分分析的开源软件风险如何分析?

成分分析基于静态风险检测，会对用户上传的软件包/固件进行解压并分析其中的文件，识别包中文件包含的开源软件清单，并分析是否存在已知漏洞、License合规等风险。用户扫描完成后，建议按照以下步骤进行分析排查：

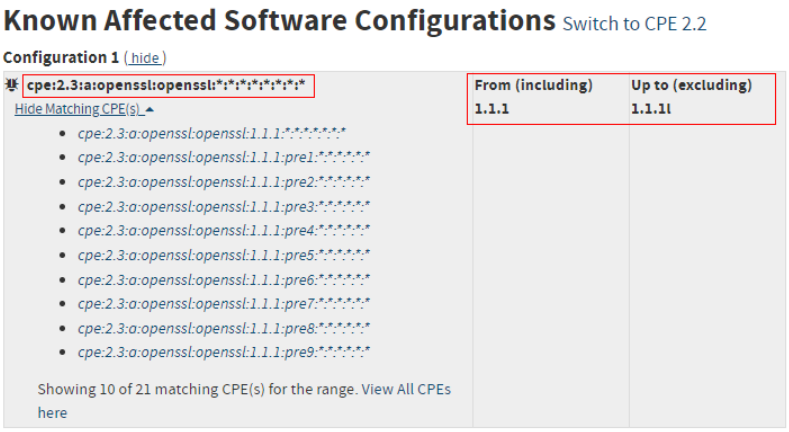
1. 开源软件分析，分析开源软件是否存在以及软件版本是否准确。

   基于报告详情页面或导出的报告中开源软件所在文件全路径找到对应文件，然后分析该文件中开源软件是否存在或准确（可由相关文件的开发或提供人员协助分析），如果否，则无需后续分析。

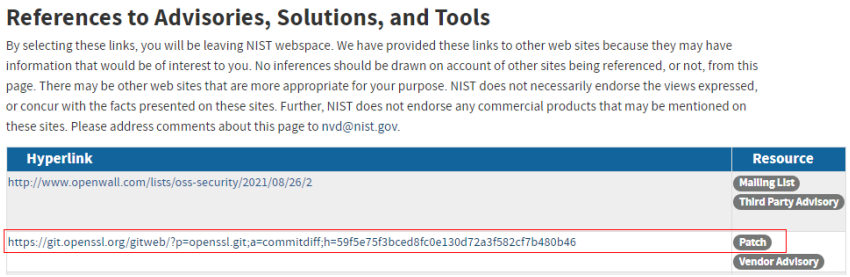
2. 已知漏洞分析，分析已知漏洞是否准确。

   通过NVD、CVE、CNVD等社区搜索相关CVE已知漏洞编号，获取漏洞详情

   - **概要分析：**查看影响的软件范围，如CVE-2021-3711在NVD社区中的Known Affected Software Configurations，如下图，确认漏洞是否影响当前使用的软件版本，如果当前使用的软件版本不在影响范围内，则初步说明漏洞可能不涉及/影响。



- **精细化分析：**漏洞通常存在于某些函数中，可以通过社区中的漏洞修复补丁确认漏洞详情、涉及函数以及修复方式，如下图，用户可以结合自身软件对于相关开源软件功能的使用是否涉及相关漏洞



3. License合规分析。基于报告中开源软件及对应的License分析软件是否合规，满足公司或准入要求。
4. 风险解决方式：
   - **已知漏洞**：如果当前使用的软件版本存在漏洞，可通过升级软件版本至社区推荐版本解决。紧急情况下也可以通过社区推荐的patch修复方式临时解决。
   - **License合规**：如果使用的软件存在合规风险，则需要寻找相似功能且合规的开源软件进行替代。

1.5 成分分析的安全编译选项类问题如何分析?

成分分析会检查用户包中的C/C++、Go文件在构建编译过程中是否添加了保护性的编译选项，来保护文件运行时免受到攻击者的攻击。

安全编译选项类问题分析指导：

1. 导出Excel报告，查看安全编译选项Sheet页。
2. 根据filepath列寻找目标文件在扫描包中位置，确认文件来源。
3. 查看目标文件对应的安全编译选项结果。
   - 如果对应项结果底色为绿色或结果值为“YES”或“NA”（rpath项禁选结果值为“No”或“NA”），则说明目标文件满足安全编译选项要求，无需处理。
   - 对于不满足要求的项，排查目标文件的构建脚本，添加对应的编译选项，其中Ftrapv和FS两项由于可能影响性能，请根据实际情况确认是否添加对应选项。

表 1-1 安全编译选项检查项参考说明

检查项	检查项描述	安全编译选项参数
BIND_NOW	立即绑定	-Wl,-z,now
NX	堆栈不可执行	-Wl,-z,noexecstack
PIC	地址无关	-fPIC
PIE	随机化	-fPIE或-pie
RELRO	GOT表保护	-Wl,-z,relro

检查项	检查项描述	安全编译选项参数
SP	栈保护	-fstack-protector-strong或-fstack-protector-all
NO Rpath/Runpath	动态库搜索路径（禁选）	脚本中删除--rpath
FS	Fortify Source(缓冲区溢出检查)	-D_FORTIFY_SOURCE=2
Ftrapv	整数溢出检查	-ftrapv
Strip	删除符号表	-s

1.6 成分分析的安全配置类问题如何分析?

成分分析会检测用户包中一些安全配置项是否合规，主要如下：

- 用户上传的软件包/固件中存在的敏感文件，如（密钥文件，证书文件，源码文件，调试工具等）。
- 用户上传的软件包/固件中操作系统中的用户与组配置、硬编码凭证、认证和访问控制等配置类问题。若不存在操作系统，则不涉及。

安全配置类检查问题分析指导：

导出PDF报告，搜索【安全配置检查概览】关键字，可以看到各检查项的结果，pass表示通过，failed表示未通过，NA表示不涉及（若无操作系统，则针对操作系统配置检查项为不涉及）。搜索【安全配置检查】关键字，可以查看具体每项的检查结果。

检查结果说明：

- 审视项：检查的方式/方法。
- 问题：存在问题的文件列表，若无问题则显示暂无问题。
- 建议值：针对检查出的问题给出的修改建议。
- 描述：审视项描述。

1.7 成分分析的信息泄露问题如何分析?

成分分析基于静态风险检测，会对用户上传的软件包/固件进行解压并分析其中的文件，识别包中是否存在信息泄露类风险，如敏感IP、GIT/SVN仓、弱口令、硬编码密钥等风险。

针对已识别的信息泄露类风险，可以通过查看导出报告中的告警详情，如PDF报告，可以在结果概览中确认是否有信息泄露风险。如果有，则可以查看相应信息泄露明细，每个告警都会包含以下几个说明，针对工具扫描出的风险清单，用户可以基于自身实际使用情况判断是否有信息泄露风险，如存在，则采取不同措施屏蔽或修改即可。

- 问题类型：IP泄露/硬编码密码/Git地址泄露等。
- 文件路径：发现信息泄露的文件在包中的全路径。
- 上下文内容：发现风险的文本行内容，包含风险内容和上下文内容。

- 匹配内容：实际发现的风险内容。
- 匹配位置：在文件中x行，x位置发现的信息泄露风险。

1.8 组件版本为什么没有被识别出来或识别错误?

成分分析扫描无法识别组件版本常见原因有：

1. 成分分析特征库不支持该开源软件版本。
2. 用户引用的开源软件修改过源码，或使用时部分引用该软件功能，导致实际编译/发布文件中相关软件特征未达到工具识别阈值，造成开源软件无法识别或版本识别异常。
3. 用户使用的开源软件包含被动依赖软件，该依赖软件可能为部分引用，造成软件无法识别或版本识别异常。

1.9 成分分析的资源包为什么购买失败了?

可能是因为权限不足导致购买失败，请检查用户权限。

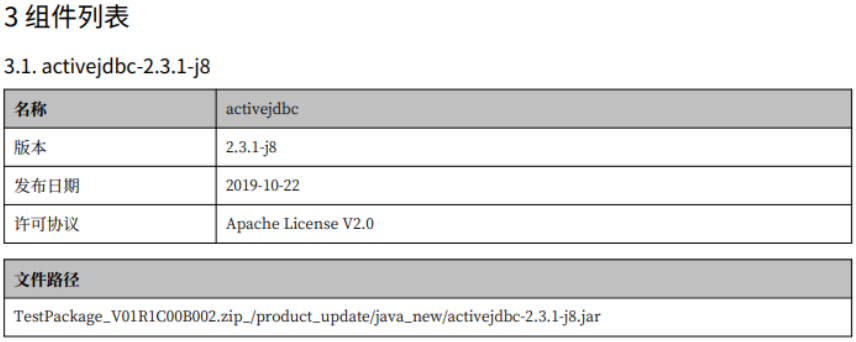
用户需要拥有te_admin、bss_adm、bss_pay或bss_ops权限才能购买开源治理服务。如需开通该权限，请联系拥有Tenant Administrator权限的用户，开通权限，详细内容请参见《**统一身份认证服务用户指南**》。

1.10 成分分析的开源漏洞文件路径如何查看?

有多种方式可查看开源漏洞分析结果的文件路径：

- 方式一：进入报告详情页面，打开开源漏洞分析扫描结果，单击“组件名称”可查看包含组件的文件对象，鼠标放在相应“对象路径”，即可查看该对象路径，也可单击右侧按钮复制；

- 方式二：打开报告详情页面，单击“下载报告 > 生成PDF报告”，待文件生成后单击“导出PDF”下载报告至本地，查阅PDF报告中第3章节，即可查看相应组件文件路径。



3 组件列表

3.1. activejdbc-2.3.1-j8

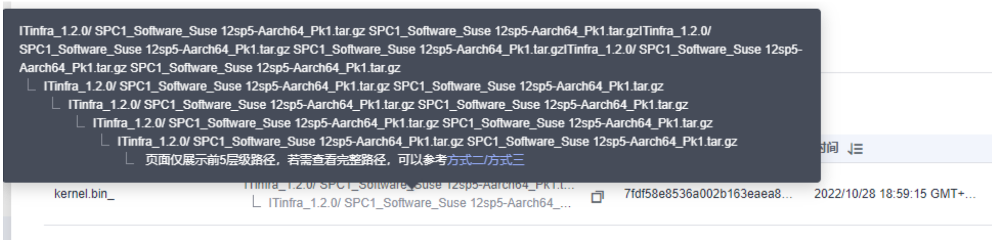
名称	activejdbc
版本	2.3.1-j8
发布日期	2019-10-22
许可协议	Apache License V2.0

文件路径
TestPackage_V01R1C00B002.zip_/product_update/java_new/activejdbc-2.3.1-j8.jar

- 方式三：打开报告详情页面，单击“下载报告”，“生成Excel报告”，待文件生成后单击“导出Excel”下载报告至本地，查阅Excel报告中“组件报告”或“漏洞报告”sheet页，即可查看相应组件文件路径。

  对象路径以“/”标识目录结构，其中“_/”表示服务对该层文件进行解析，进而分析其子目录文件。比如：scrm-service-weixin.jar_/BOOT-INF/classes/libWeWorkFinanceSdk_Java.so，您可以对scrm-service-weixin.jar进行解压缩，查看其子目录BOOT-INF/classes/libWeWorkFinanceSdk_Java.so文件，进而分析该文件中开源软件是否存在或准确。

  若文件有多个层级，则表示服务对父层级文件进行解析，进而分析子层级文件是否引用开源软件。对于方式一，多层级效果以换行缩进形式呈现，如下图所示；对于方式二或方式三，多层级路径以“:”连接展示。



1.11 成分分析的任务扫描失败怎么办?

任务扫描失败可能由多种原因造成，需要针对具体情况进行分析，常见的失败原因如下：

表 1-2 常见失败原因分析

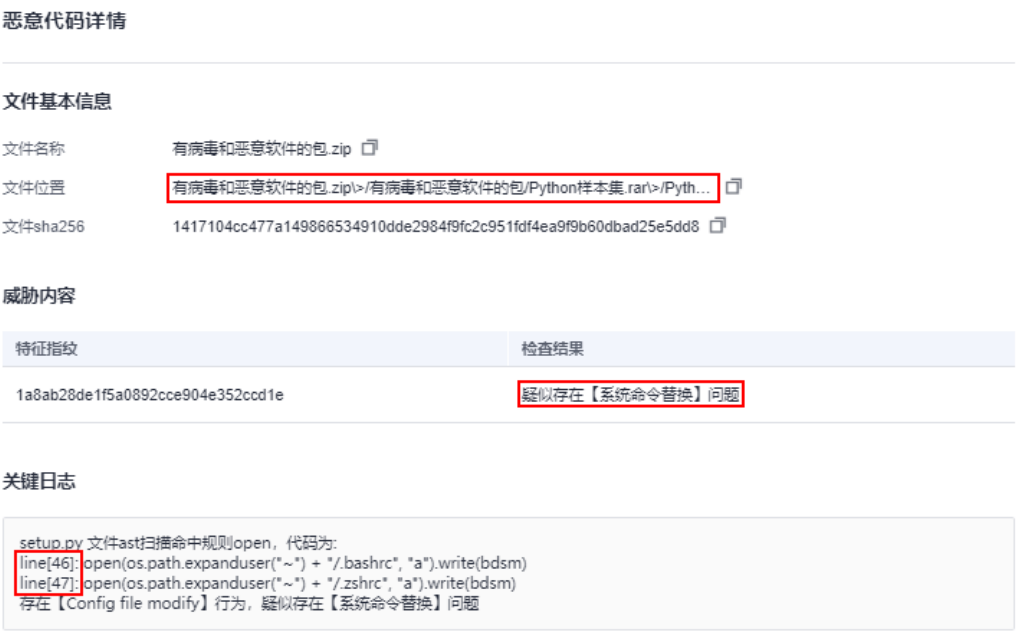
失败原因	解决方案
文件解析异常	文件本身存在不完整、结构异常等问题，导致服务无法正常解析。提供通用的压缩、固件、包格式文件重新创建扫描任务即可。
文件上传中损坏	文件在传送过程中损坏，导致无法正确解析。重新创建扫描任务进行扫描即可。
其它原因导致任务失败	多次重复创建任务后扫描任务仍然失败，可联系服务运维团队。

注意

若用户使用“按需套餐包”创建正式版任务，如果任务扫描失败，不会扣除套餐包配额；若用户使用免费版配额创建免费版任务，如果任务扫描失败，不会扣除免费版配额。

1.12 扫描到恶意代码如何定位?

进入报告详情页面，打开恶意软件扫描结果，单击“文件名称”打开恶意代码详情，可以查看告警文件位置和扫描的恶意检测结果，可以通过关键日志定位具体告警位置。



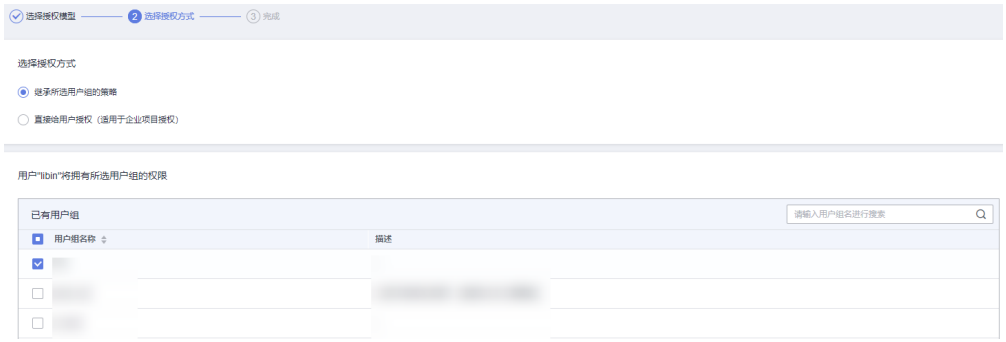
1.13 如何解决 Roles with READONLY_USER 或其他角色权限报错问题?

用户需要具有Tenant Administrator或VSS Administrator权限才能使用二进制成分分析相关业务，请分别联系具有Tenant Administrator或VSS Administrator权限的用户进行授权，可参考**如何查看用户组是否具有Tenant Administrator或VSS Administrator权限，及如何对用户组进行授权?** 查看具有权限的用户。

1. 使用具有Tenant Administrator或VSS Administrator权限的账号登录华为云，在右上角单击“控制台”。
2. 鼠标移动至右上方的账号名，在下拉列表中选择“统一身份认证”。

3. 选择待授权的用户，单击“授权”。

4. 进入“选择授权方式”步骤，选择“继承所选用户组的策略”，然后勾选具有Tenant Administrator或VSS Administrator权限的用户组。



5. 单击“确定”完成授权。

1.14 如何查看用户组是否具有 Tenant Administrator 或 VSS Administrator 权限，及如何对用户组进行授权?

1. 登录华为云，在右上角单击“控制台”。
2. 鼠标移动至右上方的账号名，在下拉列表中选择“统一身份认证”。

3. 选择“用户组”，单击用户组名称即可查看角色授权记录。

说明

切换至“用户管理”页签，可以查看该用户组下的所有用户，也可以将其他用户添加至该用户组。

4. 如果该用户组缺少相应角色权限，单击“授权”，进入“选择策略”步骤，模糊搜索“Tenant Administrator”或“VSS Administrator”权限的关键字，勾选相应策略。
5. 单击“下一步”，设置最小授权范围，然后单击“确定”，即可完成用户组角色授权。